CLAIMS

We claim:

1. A system for ensuring the identity and travel privileges of potential travelers, comprising:

a. at least one institution for researching and recording an identity and at least one travel privilege for individuals;

b. at least one database maintained by the institution for associating identified individuals' names, an assigned asymmetric key pair, and the at least one travel privilege, said at least one travel privilege including:

i. at least one destination restriction;

ii. at least one date and time restriction;

iii. at least one mode of transportation restriction;

iv. at least one operator restriction; and

v. an expiration date for each at least one travel privilege;

c. at least one travel privilege certificate associated with the at least one travel privilege and further associated with an identified individual; and

d. at least one personal identification device including a means for enrolling and authenticating individuals and managing travel privilege certificates.

2. The system described in Claim 1, wherein the travel privilege certificate comprises:

a. a name field, comprising the identified individual's full name;

b. a date field, comprising a date when the identified individual is allowed to travel;

c. a time field, comprising a time when the identified individual is allowed to travel;

d. a mode of transportation field, comprising a list of the modes of transportation that the identified individual is allowed to employ;

e. a type of privilege field, comprising the type of privilege signified by the travel privilege certificate;

f. an issue date field, comprising the date when the travel privilege certificate is issued;

g. an expiration date field, comprising the date when the travel privilege certificate is no longer valid;

h. a unique serial number; and

i. a digital signature created by the issuer of the travel privilege certificate.

3. The system described in Claim 2 wherein the list of the modes of transportation includes at least one mode selected from the group consisting of a train, a bus, a car, an airplane and a ship.

4. The system described in Claim 2 wherein the type of privilege is selected from the group consisting of a reservation ticket, a boarding pass, a port-of-entry permission and a vehicle operator permission.

5. The system described in Claim 1 wherein the database is formed by completing the following steps for each individual:

a. collecting a digital representation of the individual's handwritten signature;

b. collecting a digital photograph of the individual's face;

c. collecting a digital fingerprint template of the individual's fingerprint;

d. collecting personal identification credentials from the individual, including a birth certificate and a social security number;

e. verifying the identity of the individual by the following steps:

i. submitting the collected digital fingerprint template to the Federal Department of Criminal Justice database for review;

ii. submitting the collected birth certificate to the National Association of Public Health Services Information System database for review;

iii. submitting the collected social security number to the social security number database for review;

iv. submitting the individual's name and the collected social security number to the Immigration and Naturalization Service database for review;

v. submitting the individual's name and the collected digital photograph to a database of already-enrolled individuals' names and photographs for review;

j. determining if the individual is authorized to travel;

k. determining authorized destinations for the individual;

l.. determining authorized travel times and durations for the individual;

m. determining authorized modes of transportation for the individual;

n. creating a digital certificate and an asymmetric key pair for the individual; and

o. adding the individual's name, the collected digital photograph, public key, a date-of-validity, and the determined privileges to the database of already-enrolled individuals.

6. The system described in Claim 1 wherein the means for enrolling and authenticating individuals and managing travel privilege certificates, comprises:

a. first download means for downloading at least one travel privilege certificate to said personal identification device;

b. transmission means for transmitting at least one travel privilege certificate from said personal identification device;

c. recording means for recording at least one notable event on said personal identification device;

d. first storage means for storing at least one travel privilege certificate on said personal identification device; and

e. second storage means for storing at least one application audit log on said personal identification device.

7. The system described in Claim 6, further comprising:

a. verification means for verifying an individual's personal identity prior to issuing the travel privilege certificate;

b. second download means for downloading a computing mechanism onto the personal identification device; and

c. third download means for downloading a digital certificate and asymmetric key pair for the individual into the personal identification device.

8. The system described in Claim 6 wherein an individual's request to complete a travel-related action is evaluated and fulfilled by the following steps:

a. authenticating the individual to the personal identification apparatus;

b. verifying the date-of-validity of a stored digital certificate;

c. accessing a database of enrolled individuals, associated privileges, and public keys, and verifying the individual's ownership of the private key;

d. viewing the individual's assigned privileges in the database;

e. determining if the individual has at least one of any pre-existing notations, restrictions and provisos preventing the requested action;

f. determining additional, action-specific notations, restrictions and provisos;

g. creating a travel privilege certificate;

h. receiving the travel privilege certificate; and

i. storing the travel privilege certificate.

9. The system described in Claim 6 wherein the at least one travel privilege certificate is transmitted by the following steps:

a. authenticating the individual to the personal identification apparatus;

b. verifying the date-of-validity of a stored digital certificate;

c. accessing a database of enrolled individuals, associated privileges, and public keys, and verifying the individual's ownership of the private key;

d. selecting the at least one travel privilege certificate for transmission;

e. digitally signing the at least one travel privilege certificate with a stored private key; and

f. transmitting the signed travel privilege certificate.

10. The system described in Claim 2 wherein the mode of transportation is a motor vehicle operated by the individual and further comprising a means for verifying the individual's motor vehicle operator privileges during vehicle operation.

11. The system described in Claim 10 wherein the individual's motor vehicle operator privileges are verified at regular and pre-defined time intervals.

12. The system described in Claim 10 wherein the individual's motor vehicle operator privileges are verified at random time intervals.

13. The system described in Claim 10 wherein the individual's motor vehicle operator privileges are verified at regular and pre-defined mileage intervals.

14. The system described in Claim 10 wherein the individual's motor vehicle operator privileges are verified at random mileage intervals.

15. The system described in Claim 10 wherein the motor vehicle is disabled if verification is not achieved.

16. The system described in Claim 10 wherein the means for verifying the individual's motor vehicle operator privileges during vehicle operation is a transponder located within the motor vehicle.

17. The system described in Claim 16 wherein the transponder is connected to a local kill switch for disabling the vehicle, and receives messages from a remote institution for enabling said kill switch.

18. The system described in Claim 10 further comprising:

a. a cradle for securing the personal identification device into a specific location within the motor vehicle;

b. an electrical power connector coupled to the cradle for supplying electric power to the personal identification device, further adapted to allow the personal identification device to be fully powered and to override existing battery power; and

c. a data link connector coupled to the electrical power connector, for relaying communications between the personal identification device and a vehicle-based transponder.

19. The system described in Claim 18, wherein the cradle is secured to a motor vehicle element selected from the group consisting of a vehicle gearshift lever, a vehicle steering apparatus, a vehicle transponder and a vehicle handbrake apparatus.

20. A system for monitoring and verifying the identity of a traveling individual, comprising:

a means for collecting identification information for each traveling individual, wherein the collected identification information includes at least one biometric characteristic for the individual;

a means for verifying the collected identification information;

a means for determining at least one travel privilege for the traveling individual;

a means for creating an electronic travel privilege certificate based on the determined at least one travel privilege;

a personal identification device;

a means for transmitting the electronic travel privilege certificate to the personal identification device; and

a means for reading the electronic travel privilege certificate from the personal identification device as necessary during the traveling individual's travel.